



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,785	06/29/2001	Kenji Ohkuma	210580US2SRD	4586
22850	7590	11/29/2005	EXAMINER	
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			DAVIS, ZACHARY A	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/893,785	OHKUMA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 August 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1,4-6 and 8-18 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1,4-6 and 8-18 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.
 

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_

**DETAILED ACTION**

1. An amendment was received on 29 August 2005. Claims 1, 4-6, 8, 10, and 12-18 have been amended. Claims 2, 3, and 7 have been canceled. No new claims have been added. Claims 1, 4-6, and 8-18 are currently pending in the present application.

***Response to Arguments***

2. Applicant's arguments filed 29 August 2005 have been fully considered but they are not persuasive.

In reference to the rejection of Claims 1, 4-6, 8, 9, 11, and 14-18 under 35 U.S.C. 102(b) as anticipated by Delayaye et al, US Patent 4751733, and the rejection of Claims 10, 12, and 13 under 35 U.S.C. 103(a) as unpatentable over Delayaye in view of Matsui et al, US Patent 6201869, Applicant argues that the cited prior art does not teach or suggest all of the limitations disclosed in independent Claims 1, 4, and 12-18. Specifically in reference to Claim 1 (and by extension, in reference to all of the independent Claims), Applicant argues that Delayaye does not disclose that the first units and second unit "connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths". Applicant argues that Delayaye instead only shows that each bit is connected to one other bit via one path, referring to Figures 5 and 6.

However, there appears to be an inconsistency in the claim language and the description of the invention provided in the current response (see pages 16-17). Specifically, Applicant states that, as per Figure 35 of the present application, an S-box (a “first unit”) and a succeeding S-box (a “corresponding first unit in the succeeding encryption section”) are interconnected by two paths, and other S-boxes are interconnected by two to four paths. This is contrasted with previously known methods as depicted in Figure 36 of the present application where a first S-box is connected to a succeeding S-box by one path. However, this contradicts the claimed limitation of an “input bit terminal” being connected to a corresponding input bit terminal by at least two paths. That is, the claimed limitation appears to require individual (single) input bit terminals of the S-box to be literally connected by multiple paths, as opposed to the description in the remarks where the S-boxes as whole units are connected by multiple paths. Although the claim language appears to contradict what, by Applicant’s description, the claims are intended to encompass, for the purposes of advancing the prosecution of the present application, the claims have been examined (and were examined previously) as though they recited the intended limitations, in anticipation of the claims being amended to be brought in compliance with 35 U.S.C. 112, second paragraph (see rejections below).

Therefore, in light of the above, the Examiner believes that Delayaye does, in fact, disclose that each S-box is connected to a succeeding S-box by at least two paths. In particular, the Examiner notes that, in Figure 1, several substitution memories (corresponding to the S-boxes, or claimed “first units” or “first nonlinear transformation

units") provide input to each permutation circuit (corresponding to the diffusion units). Examples of the permutation circuits are given in Figures 5 and 6 (as noted by Applicant), and the Examiner notes that each group of 8 bits is output from a different substitution memory or S-box. Therefore, per Figures 5 and 6, Delayaye discloses that each S-box connects to each succeeding S-box by multiple paths.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
4. Claims 1, 4-6, and 8-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "to diffuse data output from the first units with respect to the first size" in lines 7-8 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the "size" is intended to affect. This renders the claim indefinite. The claim further recites the limitation "to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit ... via at least two paths" in lines 10-13 of the claim. This appears to be inconsistent with the description

provided in the current response (pages 16-17); specifically, the description in the remarks states that S-boxes (corresponding to the “first unit” of the claim) are interconnected by two to four paths. This is in contrast to the claim language, which appears to recite that individual bit input terminals of the S-boxes are literally connected by multiple paths, as opposed to the S-boxes as a whole connected by multiple paths. This contradiction renders the claim indefinite.

Claim 4 recites the limitation “perform a linear diffusion process … with respect to the first size” in at page 3, lines 4-6, of the present response. The claim further recites the limitation “perform a linear diffusion process … with respect to the second size”. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. The claim further recites the limitation “to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units … via at least two paths” at page 3, lines 17-21. This appears to be inconsistent with the description provided in the current response (pages 16-17); specifically, the description in the remarks states that S-boxes (corresponding to the “first nonlinear transformation units” of the claim) are interconnected by two to four paths. This is in contrast to the claim language, which appears to recite that individual bit input terminals of the S-boxes are literally connected by multiple paths, as opposed to the S-boxes as a whole connected by multiple paths. This contradiction renders the claim indefinite.

Claim 5 recites the limitation “input bit terminals of a second non-linear transformation unit are connected to input bit terminals of a corresponding second nonlinear transformation unit … via at least two paths” in lines 2-4 of the claim, and Claim 6 recites the limitation “input bit terminals of more than one of the second nonlinear transformation units are connected to input bit terminals of corresponding second nonlinear transformation units … via at least two paths” in lines 2-4 of the claim. This appears to be inconsistent with the description provided in the current response, as detailed above regarding Claim 4, which renders the claims indefinite.

Claim 12 recites the limitations “the first size” at page 7, line 3 of the present response, “the last stage” at page 7, line 7, and “the second size” at page 7, line 18. There is insufficient antecedent basis for these limitations in the claim. Further, the claim recites the limitations “perform a linear diffusion process … with respect to the first size” at page 7, lines 1-3, and “perform a linear diffusion process … with respect to the second size” at page 7, lines 16-18. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. The claim further recites the limitation “to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units … via at least two paths” at page 7, lines 25-28. This appears to be inconsistent with the description provided in the current response, as detailed above regarding Claim 4, which the claim indefinite.

Claim 13 recites the limitations “the first size” at page 9, line 22 of the present response, “the last stage” at page 9, line 26, and “the second size” at page 10, line 6. There is insufficient antecedent basis for these limitations in the claim. The claim further recites “the four first nonlinear transformation units” at page 9, lines 21-22. There is insufficient antecedent basis for this limitation, although it appears that this could be intended to refer instead to the two first nonlinear transformation units. Further, the claim recites the limitations “perform a linear diffusion process … with respect to the first size” at page 9, lines 20-22, and “perform a linear diffusion process … with respect to the second size” at page 10, lines 4-6. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. The claim further recites the limitation “to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units … via at least two paths” at page 9, lines 13-16. This appears to be inconsistent with the description provided in the current response, as detailed above regarding Claim 4, which the claim indefinite.

Claim 14 recites the limitation “diffusing the randomized data with respect to the first size” in line 4 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. Further, the limitation “at least one bit input to the randomizing operation is reflected on one bit input to the next randomizing operation via at least two paths” in lines 6-8 of the claim is generally vague,

as it is unclear how the bits are “reflected”. It is noted that the term “reflect” does not appear anywhere in the disclosure outside of claims 14, 15, 17, and 18. It is also unclear whether the at least one bit is reflected via at least two paths, or whether one bit is input to the next randomizing operation via at least two paths.

Claim 15 recites the limitation “to diffuse the randomized data with respect to the first size” in lines 6-7 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. Further, the limitation “at least one bit input to the randomizing operation is reflected on one bit input to the next randomizing operation via at least two randomizing and diffusing paths” in lines 10-12 of the claim is generally vague, as it is unclear how the bits are “reflected”. It is noted that the term “reflect” does not appear anywhere in the disclosure outside of claims 14, 15, 17, and 18. It is also unclear whether the at least one bit is reflected via at least two paths, or whether one bit is input to the next randomizing operation via at least two paths.

Claim 16 recites the limitation “to diffuse data output from the first units with respect to the first size” in lines 7-8 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. The claim further recites the limitation “to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit … via at least two paths” in lines 10-13 of the claim. This appears to be inconsistent with the description

provided in the current response, as detailed above regarding Claim 1, which renders the claim indefinite.

Claim 17 recites the limitation “diffusing the randomized data with respect to the first size” in line 5 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. Further, the limitation “at least one bit input to the randomizing operation is reflected on one bit input to the next randomizing operation via at least two paths” in lines 7-9 of the claim is generally vague, as it is unclear how the bits are “reflected”. It is noted that the term “reflect” does not appear anywhere in the original disclosure outside of claims 14, 15, 17, and 18. It is also unclear whether the at least one bit is reflected via at least two paths, or whether one bit is input to the next randomizing operation via at least two paths.

Claim 18 recites the limitation “to diffuse the randomized data with respect to the first size” in lines 6-7 of the claim. It is unclear exactly how data is diffused with respect to a size. That is, it is not clear what parameter or aspect of diffusion of data that the “size” is intended to affect. This renders the claim indefinite. Further, the limitation “at least one bit input to the randomizing operation is reflected on one bit input to the next randomizing operation via at least two randomizing and diffusing paths” in lines 10-12 of the claim is generally vague, as it is unclear how the bits are “reflected”. It is noted that the term “reflect” does not appear anywhere in the original disclosure outside of claims 14, 15, 17, and 18. It is also unclear whether the at least one bit is reflected via at least

two paths, or whether one bit is input to the next randomizing operation via at least two paths.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 4-6, 8, 9, 11, and 14-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Delayaye et al, US Patent 4751733.

In reference to Claim 1, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a unit to randomize subblock data obtained by dividing block data and a unit to diffuse data output from the randomizing unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of substitution memories providing input to several succeeding units through the diffusing/permuation circuits).

In reference to Claim 4-6, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a first nonlinear transformation unit and a first linear diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of

substitution memories providing input to several succeeding units through the diffusing/permuation circuits). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations).

In reference to Claim 8, Delayaye further discloses that the blocks can be 128 bits in length with subblocks of 32 bits (column 2, lines 20-32, where a block size of 32 bits is easily increased, noting that four 32 bit blocks results in a 128 bit block).

In reference to Claims 9 and 11, Delayaye further discloses implementing the diffusion unit in hardware (note the memories in Figure 1) or software (the memories may be programmable, column 5, lines 54-56).

Claims 14 and 15 are directed to a method and a software implementation, respectively, of the apparatus of Claim 1, and are rejected by a similar rationale.

Claim 16 is directed to a decryption apparatus which merely performs the reverse function of the encryption apparatus of Claim 1, and is rejected by a similar rationale, further noting that Delayaye discloses that the same device may be used for enciphering and deciphering (column 3, lines 42-46). Claims 17 and 18 are directed to a method and a software implementation, respectively, of the apparatus of Claim 16, and are rejected by a similar rationale.

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 10, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Delayaye in view of Matsui et al, US Patent 6201869.

In reference to Claim 10, Delayaye discloses everything as applied to Claim 9 above. However, Delayaye does not explicitly disclose that the diffusion unit is based on multiplication over a Galois field. Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

In reference to Claims 12 and 13, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes first nonlinear transformation unit and a first diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of substitution memories providing input to several succeeding units through the

diffusing/permuation circuits). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations, and further noting that the orders of operations can be changed and that operations can be carried out in several steps). Although Delayaye does not explicitly disclose the block sizes of 128 or 64 bits of Claims 12 and 13 respectively, Delayaye states that the block size may be changed (column 2, lines 20-32). Further, although Delayaye does disclose using the key in the substitution boxes (see Figure 1), Delayaye does not explicitly disclose key addition units. Delayaye also does not explicitly disclose the use of an operation based on multiplication over a Galois field.

Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Matsui further discloses the use of key addition units (the key is used at the XOR circuits, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field and including the key addition units, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

***Conclusion***

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*zad*  
zad

*E. Moise*  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER